FREE CISO RESOURCE

THE CISO 90-DAY PLAYBOOK

Your First 90 Days: Listen, Map, Triage, and Build the Coalition Before You Build the Strategy

---

By Dr. Erdal Ozkaya

CISO · NATO Cybersecurity Advisor · 17-time Microsoft MVP
Author of 26 cybersecurity books
erdalozkaya.com

Why this playbook exists

Most new CISOs make the same mistake in their first 90 days: they show up with the plan they wrote during the interview process and start executing it. That plan was built without the operational truth of the organisation — its actual threat profile, its tooling debt, the politics around the security function, the existing relationships that work and don't work. Executing that plan on day one is how you spend political capital you haven't yet earned, on initiatives that may not be the right ones.

The first 90 days are not about strategy. They are about earning the right to set strategy. You earn that right by listening more than you speak, by mapping the actual landscape rather than the org-chart version of it, by triaging genuine risk from political theatre, and by building a coalition that will still be with you when month four arrives and the hard decisions land.

This playbook is the framework I've used personally, refined across multiple CISO roles in three continents, and shared with hundreds of CISOs through the Global CISO Forum. It is opinionated. It assumes you are walking into a real organisation with existing tech debt, existing relationships, and an existing risk posture you did not create. It will not work as a template you mechanically execute — but the structure holds across nearly every CISO transition I've seen succeed.

THE BIG IDEA

Days 1-30 you spend almost entirely listening. Days 31-60 you deliver visible quick wins to earn credibility. Days 61-90 you turn that credibility into a board-approved 12-month plan. Skip stages at your peril.

Phase 1 — Days 1 to 30: Listen, Map, Triage

The first 30 days is where the most common CISO failure happens: feeling pressured to deliver visible action immediately, the new CISO announces an initiative, picks a fight, or fires a tool — all before understanding the terrain. Resist.

Your job in this phase is to produce three artefacts: a stakeholder map, a current-state assessment, and a triaged risk view. Nothing else.

Week 1: Land softly, set the listening frame

- Meet your team in 1:1s before any group meeting. Each person gets 30-45 minutes. Open with: "Tell me what I need to know that I won't find in the documents."
- Meet your direct manager (CIO, CEO, COO, depending on reporting line). Establish the standing meeting cadence, what success looks like to them in 6 / 12 months, and what would constitute failure.
- Request — but do not act on — the most recent: audit reports (internal and external), pen test reports, board security briefings, regulatory correspondence, incident logs.
- Walk the office floor, the data centre, and at minimum one operational site (campus, factory, branch). What you see in person disagrees with what's in the documents more often than you'd think.
- Do not announce anything. Do not commit to any initiative. Do not give anyone a date.

Week 2: Build the stakeholder map

A stakeholder map is not an org chart. It captures who actually has influence over security outcomes, including people the org chart doesn't surface.

Stakeholder type	Examples	What you need from them
Power sponsors	CEO, audit committee chair, CFO (if security spend is a board concern)	Air cover for hard decisions; signal of priority
Operational allies	CIO, CTO, Head of Infrastructure, Cloud lead, App architecture	Co-ownership of controls deployment; honest tech-debt picture
Risk peers	Chief Risk Officer, Chief Privacy / DPO, Head of Compliance, Head of Audit, Legal	Shared risk register; coordinated regulator/audit posture
Business owners	Business unit heads, product leads, sales leadership	Real understanding of business priorities; veto power over disruptive controls
External	Regulators, key vendors, IR retainer, peers in your	Calibration on what 'good' looks like in your industry

Stakeholder type	Examples	What you need from them
	sector	
Hidden influencers	Long-tenured engineers, EAs to executives, the person 'who knows everything'	Unfiltered ground truth

Week 3: Current-state inventory

By end of week 3 you should have a working document with the following sections. It does not need to be complete — it needs to be honest about what you don't yet know.

- Identity stack: IdP, MFA coverage %, privileged account count, PAM (if any), JML process state
- Endpoint: EDR coverage %, patch cadence, asset inventory completeness, contractor/BYOD posture
- Network: perimeter architecture, segmentation reality (not the diagram), egress filtering, NAC
- Cloud: providers, accounts/subscriptions inventory, posture management tooling, IaC adoption
- Application: SDLC maturity, SAST/DAST/SCA, threat modelling, secrets management, dependency risk
- Data: classification status, DLP coverage, encryption posture, data residency obligations
- Detection & response: SIEM/XDR vendor, 24/7 coverage (in-house or MSSP), IR retainer, last tabletop date
- GRC: framework alignment (NIST CSF, ISO 27001, sector-specific), policy currency, training cadence
- Resilience: BCP/DR documented vs. tested, RTO/RPO commitments, backup architecture, immutability
- Third-party: vendor count by tier, last assessment dates, fourth-party visibility
- AI/ML: AI inventory, shadow AI footprint, AI governance status, EU AI Act exposure if applicable

Week 4: Triage and triangulate

Now you compare three things: what your team says the top risks are, what the documents say the top risks are, and what your independent reading tells you. Where these three disagree is where the most important conversations happen.

AVOID THIS TRAP

Do not commit to any specific risk-rank ordering before day 30. The temptation to validate your team by accepting their risk register intact is strong. Resist until you have your own view, even if your view ends up agreeing.

Phase 2 — Days 31 to 60: Quick wins, coalition, foundation

By day 30, you've built your view of the world. Now you start spending political capital — carefully — on things that compound.

This phase has three workstreams: shipping 2-3 visible quick wins, deepening the coalition you started building in phase 1, and putting in foundational improvements that will support the 12-month plan you'll present at the end of phase 3.

Quick wins: what qualifies and what doesn't

A real quick win has three properties: it lands within 60 days, it has a visible business outcome (not just a security outcome), and a non-security audience can tell something improved. "We deployed a new SIEM rule" is not a quick win. "All 8,000 staff are now on phishing-resistant MFA, and IT helpdesk tickets related to compromised accounts dropped 70%" is.

Common quick win candidates	Typical impact	Common pitfall
Push-bombing MFA → number matching	Stops the most common 2024-26 account takeover technique	Help desk gets surprised — coordinate first
EDR rollout completion (last 5-10% of fleet)	Real coverage gap closed; visible to audit	Surfaces ghost endpoints; budget for replacements
Domain admin reduction (-50%)	Reduces blast radius dramatically; auditable	Some 'admins' may scream — have backing first
Public-facing port closure	Reduces attack surface; CISA-aligned	Inventory accuracy needed before disabling
Password expiry policy → modern (length + breached-pw screening)	Helpdesk wins; aligns to NIST 800-63B	Senior staff occasionally object; sponsor needed
Tabletop exercise (executive)	Builds IR muscle and surfaces real gaps	Risk of revealing how unprepared you are — schedule carefully
Cloud public-bucket sweep	Eliminates one common breach vector	Some buckets are intentionally public — confirm

Coalition deepening

Phase 1 mapped the coalition. Phase 2 activates it. Practically:

- Schedule a recurring 30-min slot with each of your top 6 stakeholders. Most CISOs over-rely on the CIO and CFO and under-rely on Internal Audit, Legal, and the Head of HR. The last three save your career when things go wrong.

- Establish the Security Steering Committee (or join the existing one). Make sure the agenda has both your risks and the business's priorities — not just your priorities.
- Form your IR call-tree. Run a single 30-minute call-tree drill with your CEO, CFO, CIO, Legal, and Comms. This is the cheapest tabletop you'll ever run and it pays off when the real call comes.

Foundational improvements

These are not quick wins. They are slower, deeper, less visible, and absolutely essential. Start them now so they're maturing by phase 3.

- Stand up the risk register that you and the CRO/Audit/Legal can all use. If three risk registers already exist (yours, IT's, audit's), pick the one with the strongest governance signal and feed the others into it.
- Establish the SLA for security findings: Critical 7 days, High 30 days, Medium 90 days (adjust to your context). Without this, every conversation about remediation devolves.
- Identify the two or three KPIs/KRIs that your board will see quarterly. Pick them now, even if they're imperfect. They will get better. They will only get better if they exist.
- Negotiate your IR retainer if one isn't in place. Pre-incident contracting is 5-10× cheaper than post-incident.
- If you don't have one, write your AI use policy. Adoption is already happening; the policy gives you a basis for governance.

POLITICAL CAPITAL ACCOUNTING

Track what you ask for. Every 'no' costs less if it was your only ask this month; every 'yes' compounds if it was visible. By end of phase 2, your sponsors should be able to point to two or three things they're glad you did. If they can't, you haven't shipped quick wins yet — pause foundational work and ship something visible.

Phase 3 — Days 61 to 90: Strategy, board, year-one plan

By day 60 you have credibility, a working coalition, two or three quick wins on the board, and an honest map of where the organisation is and where it needs to go. Now you convert that into the 12-month plan and brief the board.

The 12-month plan: structure

Use this skeleton. Adjust for your context but resist the urge to make it complicated.

- Mission: one sentence on what the security function exists to do — phrased in business terms, not technical.
- Three to five strategic outcomes for the year. Not initiatives — outcomes. Example: "Reduce the mean dwell time for security incidents from 12 days to under 4." Each outcome maps to several initiatives.
- Top 10 risks and their owners (not all CISO-owned). Each risk has a treatment status: accept, mitigate, transfer, avoid — and a treatment plan if mitigate or transfer.
- Roadmap by quarter, mapped to budget. Each quarter has three to five themes maximum. If you have ten themes per quarter, you don't have a plan — you have a wish list.
- KPIs and KRIs the board will see. 6-10 metrics maximum. Each one with target, current, trend, owner.
- Budget ask, broken out by run-the-bank vs. change-the-bank, with explicit trade-offs for board discretion.

The board brief

Your first board appearance as CISO is a strategic moment. Three principles.

- Brief the agenda before the meeting. Walk the audit committee chair through the deck a week before. Surprises in the boardroom cost you. Pre-aligned conversations save you.
- Twelve slides is plenty. Fifteen is too many. The board does not want depth — they want clarity and confidence.
- Open with the risk picture. Close with the ask. The middle is the plan. Pre-think the three questions you'll get from each board member.

Common phase 3 traps

TRAP 1 — The kitchen-sink board deck

You've done 60 days of intense work and want to show it. Don't. The board doesn't reward effort, they reward judgement. A deck that surfaces five things they actually need to decide on is better than a deck that surfaces 35.

TRAP 2 — Promising too much

Under-promise and over-deliver. A 12-month plan that is achievable with current resources and one quarter of contingency is more credible than one that requires every star to align. Boards remember missed commitments more than ambitious ones.

TRAP 3 — Disowning the past

Whatever was happening before you arrived is now your inheritance. Even if it was poorly managed, the board hears 'this is bad' as a critique of the people in the room. Frame your current-state assessment as forward-looking — what we're going to improve — rather than as a comparison with the past.

Deliverables checklist by phase

Print this page. Pin it where you'll see it daily.

By end of Phase 1 (Day 30)

- Stakeholder map — power sponsors, operational allies, risk peers, business owners, hidden influencers identified
- Current-state inventory — 10-domain coverage with explicit 'don't yet know' items
- Triaged risk view — your independent view triangulated with team view and document view
- Standing meetings established with manager, top 6 stakeholders, security team

By end of Phase 2 (Day 60)

- 2-3 visible quick wins delivered with measurable outcomes
- Security Steering Committee operating
- IR call-tree tested via 30-min drill
- Unified risk register agreed across security, audit, CRO
- Remediation SLAs published and accepted by IT/Engineering
- KPI/KRI shortlist (6-10) selected
- IR retainer contracted (or confirmation that current is fit for purpose)
- AI use policy published

By end of Phase 3 (Day 90)

- 12-month plan written and approved by your direct manager
- Board brief delivered (pre-aligned with audit committee chair)
- Top 10 risks with owners and treatment plans
- Quarterly roadmap with budget alignment
- First quarterly KPI/KRI report ready for next board cycle
- Personal 90-day retrospective: what worked, what surprised you, what you got wrong

Appendix A — Common failure modes

Patterns I've seen recur across CISO transitions. Recognising them early is half the defence.

The Hero Trap

New CISO tries to personally fix everything in the first 60 days. Burns out, alienates the team that needs to be doing the work, and leaves with the organisation no better than they found it. Antidote: your job is to build the capability, not to be the capability.

The Tool Reflex

Within 30 days, the new CISO is convinced they need a different SIEM / different EDR / different IdP than the one in place. Sometimes that's true. More often, the existing tool is underused, not broken. Antidote: spend the first 60 days improving how existing tools are operated before scoping replacements.

The Audit Echo Chamber

The new CISO accepts the audit findings as the priority list and starts working through them. This is comfortable because audit findings are concrete. It's also wrong — the audit reflects what auditors can measure, not necessarily what's most risky. Antidote: use audit findings as one input, not the input.

Going Big Too Early

A board-ready, ambitious 3-year strategic plan delivered at day 30. The plan looks great. It will also be wrong — because you haven't built the operational truth yet. Antidote: nothing strategic before day 60.

The Predecessor Problem

Hidden tensions from the previous CISO's tenure surface as resistance to your initiatives. Old grudges, old commitments, old workarounds. Antidote: identify these in phase 1 stakeholder conversations. Ask explicitly: "What did my predecessor do that you'd want to see continued? What would you want to see change?"

Appendix B — Further reading from this site

The full CISO Toolkit is free at https://erdalozkaya.com/ciso-toolkit/ and includes:

- Vendor Security Assessment Framework — the questionnaire used in this playbook's quick-win recommendations
- Ransomware Response Playbook — pair with your IR call-tree drill
- Zero Trust Architecture Blueprint — for the foundational network/identity work in Phase 2
- GRC Risk Register Template — for the unified risk register milestone in Phase 2
- InfoSec Policy Framework — for closing policy gaps surfaced in Phase 1 inventory
- Board Cybersecurity Presentation — template for the Day 90 board brief
- AIGF (Ozkaya AI Governance Framework) — for the AI use policy milestone in Phase 2

About the Author

Dr. Erdal Ozkaya is CISO at Morgan State University, NATO Cybersecurity Advisor, 17-time Microsoft MVP, President of the Global CISO Forum, and author of 26 cybersecurity books. He has held CISO and security architect roles at Standard Chartered Bank, Microsoft, Xcitium/Comodo, and Secunia, working across 50+ countries. He is a regular keynote speaker at RSA Conference, Black Hat, and GITEX, and contributes to NATO cybersecurity programmes. More at erdalozkaya.com.